REMARKS

This is in response to the Office Action of December 28, 2005. Consideration of this Amendment and allowance is requested in view of the amendments made to the claims.

The amendments made to independent claims 1, 14 and 15 are based on features originally claimed in now canceled claims 5 and 6. The term "lock" in the preamble has been amended to "locking cylinder" to more accurately define the invention. A corresponding change has been made in the specification.

The Examiner alleges that the invention as claimed in claims 1-9 and 12-15 was anticipated by U.S. 4,712,398 (Clarkson, et al) and that claims 10 and 11 were obvious over a combination of Clarkson et al. and US 5,447,047 (Lin et al). Reconsideration of the amended claims and allowance is respectfully requested.

In US 4,712,398 (Clarkson, et al) a key operated locking system is disclosed, which includes a mortise lock cylinder 50 in which a key 30 has to be inserted to open the lock. The mortise lock cylinder 50 comprises a cylinder control logic 100, a key centering/retention assembly 90 and a release assembly 70.

The key 30 used in the key operated locking system has at its lower edge 34 a cavity 35 in which an integrated circuit package 42 and key connectors 45 are arranged (see Fig. 1 to 4 of Clarkson, et al). The integrated circuit package 42 comprises a key memory 40 in which keying codes are stored.

When the key is inserted in the mortise lock cylinder 50, the key connectors 45, i.e. ohmic contacts 45a-d abut against cylinder connectors 59a-d, which are placed along the lower edge of the key (see col. 5, lines 24-26 and Figs. 2, 3 and 4 of Clarkson et al.). Due to the electrical contact established between the key connectors 45 and the cylinder connectors 59a-d the lock electronics 100 can receive a keying code from the key memory 40. In case a valid code is recognized by the lock electronics 100, a retraction force is applied to a pin 72 of the

release assembly 70, so that the key 30 can rotate the plug 55 of the lock cylinder 50 to open the lock.

In contrast thereto, the invention as claimed in amended independent claims 1, 14 and 15 provides a lock comprising a knob which can be actuated from the outside of the door and a deactivation member which can deactivate the knob so that the opening of the door using the knob is not possible. The lock further includes an access control means which comprises means for exchanging a wireless signal with a transponder and a verification means for verifying whether or not the transponder is authorized. In case a transponder is authorized, the access control means in response to the authorized transponder signal, permits opening of the door by making it possible for the user to actuate the knob from the outside of the door in order to open it.

This has the advantage that no cylinder comprising a keyway for inserting a key to open the lock has to be provided as disclosed in Clarkson, et al. Further, the knob as claimed provides a closed body and therefore a good protection against manipulation from outside.

In contrast thereto, the key operated locking system as shown in Clarkson, et al has several disadvantages.

In Clarkson, et al the cylinder connectors 59a-d and the key connectors 45a-d are directly accessible from the outside so that they can corrode or can get dirty or damaged. Further, the keyhole provides a direct access for an unauthorized user to manipulate the cylinder by using for example a drill to destroy the release assembly 70 or the cylinder as a whole. In particular, an unauthorized user can easily destroy the cylinder connectors 59a-d in the cylinder 50 to make the cylinder inoperable. Furthermore, the lock electronics 100 can be destroyed by applying a high voltage to the cylinder.

The claimed invention provides a knob which does not have a

keyhole and which is further operated through a wireless data exchange between a transponder and an access control means, which is entirely located within the locking cylinder body.

The wireless data exchange according to the invention as claimed avoids the above mentioned problems of Clarkson, et al, since the lock does not need key connectors which abut against cylinder connectors, when the key is inserted in the keyway of the cylinder of Clarkson et al. The invention provides instead a wireless transmission. It is respectfully submitted that there is no disclosure in Clarkson et al regarding the feature of amended independent claims 1, 14 and 15 of access control means which comprises means for exchanging a wireless signal with a transponder.

In this connection it has to be emphasized that the cylindrical connectors 59 in Clarkson, et al are electrical contacts and clearly not a ferrit bar antenna as alleged by the Examiner. Further, the key connectors 45 in Clarkson, et al are also electrical contacts and clearly not a transponder as alleged by the Examiner.

The Examiner cited col. 4, lines 51 to col. 5, line 8 of Clarkson et al as disclosing an access control means which has means for exchanging a wireless signal with a transponder and a verification means for verifying whether or not the transponder is authorized. In that interpretation of Clarkson et al. is respectfully contested the passage cited by the Examiner, it is indicated that the electronic logic circuitry 100 can extract electronically encoded information from the key memory via key connectors 45 and cylinder connectors 59. That means information from the key memory can be received when the electrical contacts of the key, i.e. key connectors 45, abut against the electrical contacts of the cylinder, i.e. the cylinder connectors 59. It is clear to a person skilled in the art, that this is completely different from the access control means as claimed which has

means for exchanging a wireless signal with a transponder. The transponder does not "abut" against the access control means for transmitting a wireless signal.

The fact that the cylinder of the lock as claimed performs a wireless data exchange has the further advantage that RFID cards (Hitag, Legic) can be used. Further, the cylinder of the lock can be online controlled, reprogrammed and read-out via, e.g., Bluetooth, Zigbee or other suitable frequencies. This is not possible with the key operated locking system as disclosed in Clarkson, et al in which the key connectors 45 have to contact the cylinder connectors 59. Thus, it is respectfully submitted that amended claims 1-9 and 14 and 15 are not anticipated by Clarkson et al.

US 5,447,047 (Lin et al) which was combined with Clarkson et al. for rejecting claims 10 and 11. The failure to teach or suggest the structure of parent claim 1 is described above. Lin et al. fails to provide a further teaching that would render claims 10 and 11 obvious. In Lin et al. a door lock is disclosed which comprises an outer housing 1, wherein a decoding means 11 is disposed in front of the outer housing and cooperated with a magnetic card, finger prints or a key board in order to energize a coil 13 to unlock a dead bolt. The dead bolt includes an outer lever 3 and an inner lever 4, wherein the coil 13 is disposed in the outer lever 3 and has two extensions. A shaft 42 is coupled between the two levers, wherein a disc is engaged on the shaft 42 and has two grooves for engaging with the extensions of a rod 52. The extensions of the rod 52 are biased away from the grooves of the disc such that the shaft 42 can not be rotated by the outer lever 3. When the coil 13 is energized the rod 52 is caused to move toward the disc such that the extensions of the rod 52 are caused to engage with the grooves of the disc and such that the shaft 42 can be rotated by the outer lever 3.

Lin et al discloses a conventional coupling mechanism via an

electromagnet, wherein the coil 13, when it is in a coupling state, is provided the whole time with energy (see col. 3, lines 33ff). Further, Lin et al does not disclose how the coil can be protected against manipulation e.g. by applying a magnetic field from the outside. The coil is arranged on the axis of the cylinder so that a longitudinal field can be easily applied from the outside.

Further, Lin et al does not disclose an access control means as claimed which comprises an access control means including means for exchanging a wireless signal with a transponder and a verification means for verifying whether or not the transponder is authorized. Instead, Lin et al provides a decoding means 11 which is disposed in front of an outer housing and which is cooperated with a magnetic card, finger prints or a key board in order to energize a coil 13 to unlock a dead bolt.

It is thus believed claims 10 and 11 are allowable with parent claim 1. The detailed action amendment claims 12 and 13 in the rejection over Clarkson et al. However, it is believed claims 12 and 13 have been withdrawn.

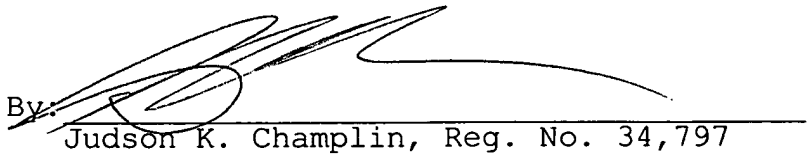
An Information Disclosure Statement citing additional references that have been uncovered in companion cases is enclosed. The fee of $180.00 is enclosed for consideration of the Information Disclosure Statement.

Thus, the applicant believes the amended claims should be allowable. Favorable action is respectfully requested.

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.



By: _____

Judson K. Champlin, Reg. No. 34,797
Suite 1400 - International Centre
900 Second Avenue South
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

JKC:lrs